



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,173	09/12/2003	ASHOT ANDREASYAN	PR 1803.01 US	2172
31883 7590 07/02/2007 DVA/PIONEER RESEARCH CENTER USA, INC. 2265 E. 220TH STREET LONG BEACH, CA 90810			EXAMINER HA, LEYNNA A	
			ART UNIT	PAPER NUMBER
			2135	
			MAIL DATE	DELIVERY MODE
			07/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/605,173	ANDREASYAN, ASHOT	
	<b>Examiner</b>	<b>Art Unit</b>	
	LEYNNA T. HA	2135	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 17 April 2007.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-35 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-35 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. Claims 1-35 have been examined and is pending.  
Claims 33-35 are new claims.
2. Claims 1-8 and 17-32 previously rejected under 35 U.S.C. 101 are now withdrawn.
3. This is a Final rejection necessitated by new grounds of rejection.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1-32 are rejected under 35 U.S.C. 102(e) as being anticipated by Roy (US 6,677,888).**

#### **As per claim 1:**

Roy discloses the method for generating a shared key comprising:

providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters, the first peer and second peer being communicated over a network; **(col.10, lines 58-64; Roy discloses the certificate**

Art Unit: 2135

**obtained of the aircraft is the claimed 1<sup>st</sup> certificate provided where the parameters being the digital signature.)**

performing a first exponentiation operation to generate a first public key from the second peer using at least one parameter of the plurality of first parameters and a first private key from the second peer, wherein the first parameters being digital signature standard parameters; (col.9, lines 44-60; Roy discloses generating by computing the public key which selects a private key and to sign a message with a known hash function (SHA-1) thereby obtaining a digital fingerprint of the message. The hash that obtains the digital fingerprint is claimed to the 1<sup>st</sup> parameters being signature standard parameters.)

providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters; (col.10, lines 27-32; Roy discloses the CA issues the public key certificates with domain parameters and the key size to determine the cryptographic strength as the claimed provided the 2<sup>nd</sup> certificate and public key with 2<sup>nd</sup> parameters.)

performing a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters; (col.10, lines 48-52; Roy discusses a secret session key is established in a request message that sends the message with the signature as the claimed shared secret key using a parameter from the first parameters. The parameter from the first parameters is referring to signature standard parameters as claimed above.)

performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer. (col.10, lines 1-9)

Roy discloses

**As per claim 2:** See col.9, lines 32-35; discussing the method according to claim 1 wherein the first certificate is a DSA type certificate.

**As per claim 3:** See col.11, lines 13-16; discussing the method according to claim 2 wherein the first and second parameters comprise a prime number  $p_{\text{sub.dss}}$ , a prime number  $q_{\text{sub.dss}}$  a generator  $g_{\text{sub.dss}}$  and a public key for the first and second peers, respectively.

**As per claim 4:** See col.9, lines 44-60; discussing the method according to claim 3 wherein the first exponentiation operation to generate the first public key is  $Y_{\text{sub.R}} = g_{\text{sub.dss}}^{\text{circumflex over ( )}} X_{\text{sub.R}} \text{ mod } p_{\text{sub.dss}}$  where  $X_{\text{sub.R}}$  is a one-time private key from the second peer.

**As per claim 5:** See col.10, lines 1-9; discussing the method according to claim 4 wherein the second exponentiation operation to generate the shared secret key for the second peer is  $_{\text{sub.SSK}} = Y_{\text{sub.Adss}}^{\text{circumflex over ( )}} X_{\text{sub.R}} \text{ mod } p_{\text{sub.dss}}$  where  $Y_{\text{sub.Adss}}$  is a DSS public key from certificate of peer A.

**As per claim 6:** See col.10, lines 1-9; discussing the method according to claim 5 wherein  $Y_{\text{sub.Adss}} = g_{\text{sub.dss}}^{\text{circumflex over ( )}} X_{\text{sub.Adss}} \text{ mod } p_{\text{sub.dss}}$  where  $X_{\text{sub.Adss}}$  is a DSS private key from certificate of peer A.

**As per claim 7:** See col.10, lines 1-9; discussing the method according to claim 5

Art Unit: 2135

wherein the third exponentiation operation to generate the shared secret key for the first peer is  $Y_{\text{sub}}.SSK = YR^{\{ \text{circumflex over ( )} \}} X_{\text{sub}}.Adss \bmod p_{\text{sub}}.dss$  where  $X_{\text{sub}}.Adss$  is a DSS private key from certificate of peer A.

**As per claim 8: See FIG.1 and col.5, lines 50-60;** discussing the method according to claim 1 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

**As per claim 9:**

Roy discloses the article of manufacture comprising:

a machine accessible medium including data that, when accessed by a machine, causes the machine to perform operations comprising: **(col.5, lines 30-46)**

providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters; **(col.10, lines 58-64; Roy discloses the certificate obtained of the aircraft is the claimed 1<sup>st</sup> certificate provided where the parameters being the digital signature.)**

performing a first exponentiation operation to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer; **(col.9, lines 44-60; Roy discloses generating by computing the public key which selects a private key and to sign a message with a known hash function (SHA-1) thereby obtaining a digital fingerprint of the message. The hash that obtains the digital fingerprint is claimed to the 1<sup>st</sup> parameters being signature standard parameters.)**

providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters; **(col.10, lines 27-32; Roy discloses the CA issues the public key certificates with domain parameters and the key size to determine the cryptographic strength as the claimed provided the 2<sup>nd</sup> certificate and public key with 2<sup>nd</sup> parameters.)**

performing a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters; **(col.10, lines 48-52; Roy discusses a secret session key is established in a request message that sends the message with the signature as the claimed shared secret key using a parameter from the first parameters. The parameter from the first parameters is referring to signature standard parameters as claimed above.)**

performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer. **(col.10, lines 1-9)**

**As per claim 10: See col.9, lines 32-35;** discussing the article of manufacture according to claim 9 wherein the first certificate is a DSA type certificate.

**As per claim 11: See col.11, lines 13-16;** discussing the article of manufacture according to claim 10 wherein the first and second parameters comprise a prime number  $p_{\text{sub.dss}}$ , a prime number  $q_{\text{sub.dss}}$ , a generator  $g_{\text{sub.dss}}$  and a public key for the first and second peers, respectively.

**As per claim 12: See col.10, lines 1-16;** discussing the article of manufacture



Art Unit: 2135

according to claim 11 wherein the first exponentiation operation to generate the first public key is  $Y_{sub.R} = g_{sub.dss} \{ \text{circumflex over ( )} \} X_{sub.R} \bmod p_{sub.dss}$  where  $X_{sub.R}$  is a one-time private key from the second peer.

**As per claim 13:** See col.10, lines 1-9; discussing the article of manufacture according to claim 12 wherein the second exponentiation operation to generate the shared secret key for the second peer is  $Y_{sub.SSK} = Y_{sub.Adss} \{ \text{circumflex over ( )} \} X_{sub.R} \bmod p_{sub.dss}$  where  $Y_{sub.Adss}$  is a DSS public key from certificate of peer A.

**As per claim 14:** See col.10, lines 1-9; discussing the article of manufacture according to claim 13 wherein  $Y_{sub.Adss} = g_{sub.dss} \{ \text{circumflex over ( )} \} X_{sub.Adss} \bmod p_{sub.dss}$  where  $X_{sub.Adss}$  is a DSS private key from certificate of peer A.

**As per claim 15:** See col.10, lines 1-9 discussing the article of manufacture according to claim 13 wherein the third exponentiation operation to generate the shared secret key for the first peer is  $Y_{sub.SSK} = Y_{sub.R} \{ \text{circumflex over ( )} \} X_{sub.Adss} \bmod p_{sub.dss}$  where  $X_{sub.Adss}$  is a DSS private key from certificate of peer A.

**As per claim 16:** See FIG.1 and col.5, lines 50-60; discussing the article of manufacture according to claim 9 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

**As per claim 17:**

Roy discloses a system comprising:



Art Unit: 2135

a processor; and a memory coupled to the processor, the memory containing program code that, when executed by the processor, causes the processor to: **(col.14, lines 61-67)**

provide a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters; **(col.10, lines 58-64; Roy discloses the certificate obtained of the aircraft is the claimed 1<sup>st</sup> certificate provided where the parameters being the digital signature.)**

perform a first exponentiation operation to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer; **(col.9, lines 44-60; Roy discloses generating by computing the public key which selects a private key and to sign a message with a known hash function (SHA-1) thereby obtaining a digital fingerprint of the message. The hash that obtains the digital fingerprint is claimed to the 1<sup>st</sup> parameters being signature standard parameters.)**

provide a second certificate and the first public key from the second peer to the first peer; the second certificate comprising a plurality of second parameters; **(col.10, lines 27-32; Roy discloses the CA issues the public key certificates with domain parameters and the key size to determine the cryptographic strength as the claimed provided the 2<sup>nd</sup> certificate and public key with 2<sup>nd</sup> parameters.)**

perform a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters; **(col.10, lines 48-52; Roy discusses a secret session key is established in a**

Art Unit: 2135

**request message that sends the message with the signature as the claimed shared secret key using a parameter from the first parameters. The parameter from the first parameters is referring to signature standard parameters as claimed above.)**

performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer. (col.10, lines 1-9)

**As per claim 18: See col.9, lines 32-35;** discussing the system according to claim 17 wherein the first certificate is a DSA type certificate.

**As per claim 19: See col.11, lines 13-16;** discussing the system according to claim 18 wherein the first and second parameters comprise a prime number  $p_{\text{sub.dss}}$ , a prime number  $q_{\text{sub.dss}}$ , a generator  $g_{\text{sub.dss}}$  and a public key for the first and second peers, respectively.

**As per claim 20: See col.9, lines 44-60;** discussing the system according to claim 19 wherein the first exponentiation operation to generate the first public key is  $Y_{\text{sub.R}} = g_{\text{sub.dss}}^{\text{circumflex-x over ( )}} X_{\text{sub.R}} \text{ mod } p_{\text{sub.dss}}$  where  $X_{\text{sub.R}}$  is a one-time private key from the second peer.

**As per claim 21: See col.10, lines 1-9;** discussing the system according to claim 20 wherein the second exponentiation operation to generate the shared secret key for the second peer is  $Y_{\text{sub.SSK}} = Y_{\text{sub.dss}}^{\text{circumflex over ( )}} X_{\text{sub.R}} \text{ mod } p_{\text{sub.dss}}$  where  $Y_{\text{sub.Adss}}$  is a DSS public key from certificate of peer A.

**As per claim 22: See col.10, lines 1-16;** discussing the system according to claim

Art Unit: 2135

21 wherein  $Y_{\text{sub}}.\text{Adss} = g_{\text{sub}}.\text{dss} \{ \text{circumflex over ( )} \} X_{\text{sub}}.\text{Adss}$  where  $X_{\text{sub}}.\text{Adss}$  is a DSS private key from certificate of peer A.

**As per claim 23:** See col.10, lines 1-9; discussing the system according to claim 21 wherein the third exponentiation operation to generate the shared secret key for the first peer is  $Y_{\text{sub}}.\text{SSK} = Y_{\text{sub}}.\text{Adss} \{ \text{circumflex over ( )} \} X_{\text{sub}}.\text{Adss} \bmod p_{\text{sub}}.\text{dss}$  where  $X_{\text{sub}}.\text{Adss}$  is a DSS private key from certificate of peer A.

**As per claim 24:** See FIG.1 and col.5, lines 50-60; discussing the system according to claim 17 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

**As per claim 25:**

Roy discloses a method comprising:

receiving a first certificate including a plurality first parameters; (col.10, lines 58-64; Roy discloses the certificate obtained of the aircraft is the claimed 1<sup>st</sup> certificate provided where the parameters being the digital signature.)

performing a first exponentiation operation to generate a first public key using at least one parameter of the plurality of first parameters and a first private key; (col.9, lines 44-60; Roy discloses generating by computing the public key which selects a private key and to sign a message with a known hash function (SHA-1) thereby obtaining a digital fingerprint of the message. The hash that obtains the digital fingerprint is claimed to the 1<sup>st</sup> parameters being signature standard parameters.)

receiving a second certificate and the first public key, the second certificate including a plurality of second parameters; (col.10, lines 27-32; Roy discloses the CA

Art Unit: 2135

**issues the public key certificates with domain parameters and the key size to determine the cryptographic strength as the claimed provided the 2<sup>nd</sup> certificate and public key with 2<sup>nd</sup> parameters.)**

performing a second exponentiation operation to generate a first shared secret key using at least one parameter from the plurality of first parameters; **(col.10, lines 48-52; Roy discusses a secret session key is established in a request message that sends the message with the signature as the claimed shared secret key using a parameter from the first parameters. The parameter from the first parameters is referring to signature standard parameters as claimed above.)**

performing a third exponentiation operation to generate a second shared secret key using the first public key and a private key. **(col.10, lines 1-9)**

**As per claim 26: See col.9, lines 32-35;** discussing the method according to claim 25 wherein the first certificate is a DSA type certificate.

**As per claim 27: See col.11, lines 13-16;** discussing the method according to claim 26 wherein the first and second parameters each comprises a prime number  $p_{\text{sub.dss}}$ , a prime number  $q_{\text{sub.dss}}$ , a generator  $g_{\text{sub.dss}}$  and a public key.

**As per claim 28: See col.10, lines 1-16;** discussing the method according to claim 27 wherein the first exponentiation operation to generate the first public key is  $Y_{\text{sub.R}} = g_{\text{sub.dss}}^{\text{circumflex-x over ( )}} X_{\text{sub.R}} \bmod P_{\text{sub.dss}}$  where  $X_{\text{sub.R}}$  is a one-time private key.

**As per claim 29: See col.10, lines 1-3;** discussing the method according to claim 28 wherein the second exponentiation operation to generate the first shared secret key for

Art Unit: 2135

the second peer is  $.sub.SSK=Y.sub.Adss \{ \text{circumflex over ( )} \} X.sub.R \text{ mod } p.sub.dss$

where  $Y.sub.Adss$  is a DSS public key.

**As per claim 30:** See col.10, lines 1-9; discussing the method according to claim 29

wherein  $Y.sub.Adss=g.sub.dss\{ \text{circumflex over ( )} \} X.sub.Adss \text{ mod } p.sub.dss$  where

$X.sub.Adss$  is a DSS private key.

**As per claim 31:** See col.10, lines 65-67; discussing the method according to claim

29 wherein the third exponentiation operation to generate a second shared secret key is

$Y.sub.SSK=Y.sub.R\{ \text{circumflex over ( )} \} X.sub.Adss \text{ mod } p.sub.dss$  where  $X.sub.Adss$  is

a DSS private key.

**As per claim 32:** See FIG.1 and col.5, lines 50-60; discussing the method

according to claim 25 wherein the first and second certificates are sent to the second

and first peers, respectively, over a wireless network.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**5. Claims 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable**

**over Roy (US 6,677,888), and further in view of Yeager, et al. (US 7,222,187).**

Art Unit: 2135

**As per claim 33:** Roy discloses an a wireless network invention (col.5, lines 50-60) that uses Elliptic Curve DSA to prevent forgery and Diffie-Hellman key agreement scheme (col.9, lines 33-35 and col.10, lines 1-3). However, Roy fails to mention the network be one of a Bluetooth network.

Yeager discloses Embodiments of a decentralized, distributed trust mechanism are described that may be used in various networking platforms, including, but not limited to, peer-to-peer and other decentralized networking platforms. The mechanism may be used, among other things, to implement trust relationships between and among peers and to implement trust relationships between peers and content and data (col.2, lines 44-50). Roy discusses the peer-to-peer platform may be independent of specific security approaches where the peer-to-peer platform may provide a comprehensive set of security primitives to support the security solutions used by various peer-to-peer platform services and applications. Embodiments of the peer-to-peer platform may provide one or more security primitives including, but not limited to: A simple crypto library supporting hash functions (e.g. MD5), symmetric encryption algorithms (e.g. RC4), and asymmetric crypto algorithms (e.g., Diffie-Hellman and RSA) (col.58, line 61 – col.57, line 4). Roy further discloses that in order to interact with other peers the peer needs to be connected to some kind of network (wired or wireless) such as, IP, Bluetooth, or Havi, among others (col.27, lines 31-35) and that peer-to-peer platform may be independent of transport protocols (col.33, lines 21-25). For example, the peer-to-peer platform may be implemented on top of TCP/IP, HTTP, Bluetooth, HomePNA and other protocols.



Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Roy with Yeager to teach a Bluetooth network because in order to interact with other peers the peer needs to be connected to some kind of network (wired or wireless) such as Bluetooth (col.27, lines 31-35) and peer-to-peer platform may be independent of transport protocols that may be implemented on top Bluetooth (col.33, lines 21-25).

**As per claim 34:** Roy discloses an a wireless network invention (col.5, lines 50-60) that uses Elliptic Curve DSA to prevent forgery and Diffie-Hellman key agreement scheme (col.9, lines 33-35 and col.10, lines 1-3). However, Roy fails to mention the network be one of a Bluetooth network.

Yeager discloses Embodiments of a decentralized, distributed trust mechanism are described that may be used in various networking platforms, including, but not limited to, peer-to-peer and other decentralized networking platforms. The mechanism may be used, among other things, to implement trust relationships between and among peers and to implement trust relationships between peers and content and data (col.2, lines 44-50). Roy discusses the peer-to-peer platform may be independent of specific security approaches where the peer-to-peer platform may provide a comprehensive set of security primitives to support the security solutions used by various peer-to-peer platform services and applications. Embodiments of the peer-to-peer platform may provide one or more security primitives including, but not limited to: A simple crypto library supporting hash functions (e.g. MD5), symmetric encryption algorithms (e.g. RC4), and asymmetric crypto algorithms (e.g., Diffie-Hellman and RSA) (col.58, line 61



Art Unit: 2135

– col.57, line 4). Roy further discloses that in order to interact with other peers the peer needs to be connected to some kind of network (wired or wireless) such as, IP, Bluetooth, or Havi, among others (col.27, lines 31-35) and that peer-to-peer platform may be independent of transport protocols (col.33, lines 21-25). For example, the peer-to-peer platform may be implemented on top of TCP/IP, HTTP, Bluetooth, HomePNA and other protocols.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Roy with Yeager to teach a Bluetooth network because in order to interact with other peers the peer needs to be connected to some kind of network (wired or wireless) such as Bluetooth (col.27, lines 31-35) and peer-to-peer platform may be independent of transport protocols that may be implemented on top Bluetooth (col.33, lines 21-25).

**As per claim 35:** Roy discloses an a wireless network invention (col.5, lines 50-60) that uses Elliptic Curve DSA to prevent forgery and Diffie-Hellman key agreement scheme (col.9, lines 33-35 and col.10, lines 1-3). However, Roy fails to mention the network be one of a Bluetooth network.

Yeager discloses Embodiments of a decentralized, distributed trust mechanism are described that may be used in various networking platforms, including, but not limited to, peer-to-peer and other decentralized networking platforms. The mechanism may be used, among other things, to implement trust relationships between and among peers and to implement trust relationships between peers and content and data (col.2, lines 44-50). Roy discusses the peer-to-peer platform may be independent of specific

Art Unit: 2135

security approaches where the peer-to-peer platform may provide a comprehensive set of security primitives to support the security solutions used by various peer-to-peer platform services and applications. Embodiments of the peer-to-peer platform may provide one or more security primitives including, but not limited to: A simple crypto library supporting hash functions (e.g. MD5), symmetric encryption algorithms (e.g. RC4), and asymmetric crypto algorithms (e.g., Diffie-Hellman and RSA) (col.58, line 61 – col.57, line 4). Roy further discloses that in order to interact with other peers the peer needs to be connected to some kind of network (wired or wireless) such as, IP, Bluetooth, or Havi, among others (col.27, lines 31-35) and that peer-to-peer platform may be independent of transport protocols (col.33, lines 21-25). For example, the peer-to-peer platform may be implemented on top of TCP/IP, HTTP, Bluetooth, HomePNA and other protocols.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Roy with Yeager to teach a Bluetooth network because in order to interact with other peers the peer needs to be connected to some kind of network (wired or wireless) such as Bluetooth (col.27, lines 31-35) and peer-to-peer platform may be independent of transport protocols that may be implemented on top Bluetooth (col.33, lines 21-25).

***Response to Arguments***

6. Applicant's arguments with respect to claims 1-35 have been considered but are moot in view of the new ground(s) of rejection.

***Conclusion***

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

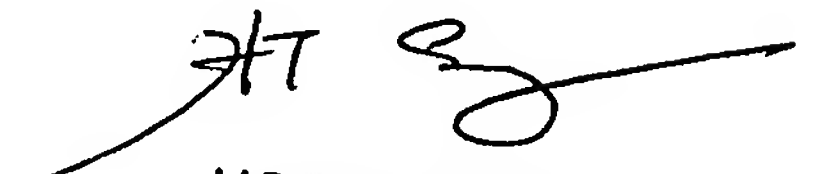
Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

  
HOSUK SONG  
PRIMARY EXAMINER